Software Assurance and the Practitioner

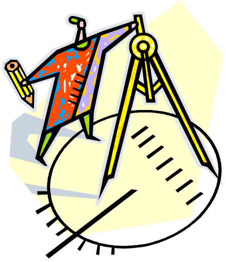
June 27, 2005

Susan Sekira

OSSMA, Software Assurance Lead

Objectives

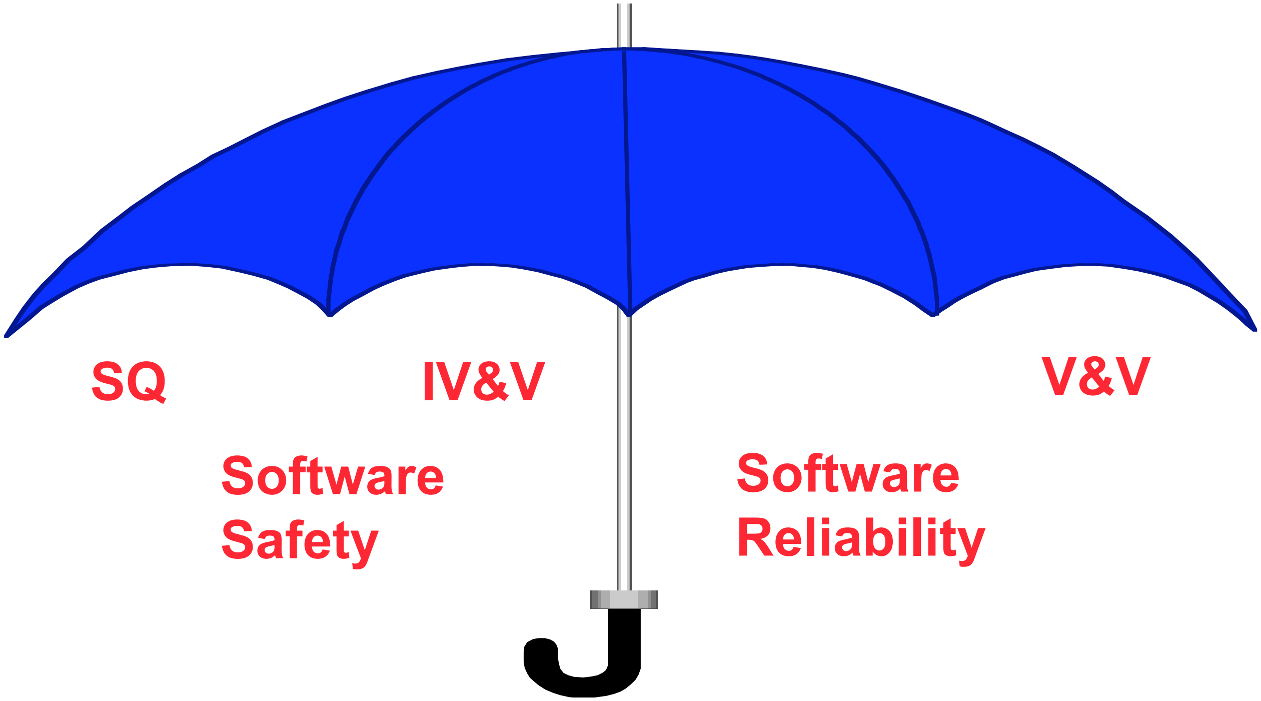
- **Establish a common framework and understanding among the GSFC software community**
  - What is Software Assurance?
  - Who are the Software Assurance practitioners?
  - Is Software Assurance the same as Software Quality?
  - What's the difference between Software Quality and IV&V?
  - How do I start a Software Assurance Program?
  - Will Software Quality help me meet the goals of CMMI?
- **Highlight the benefits of software assurance throughout the development life cycle**



General Audience: Project Managers, Software Managers, Software Engineers, Safety Engineers, and Systems Engineers

What is Software Assurance?

Software Assurance is an umbrella risk identification and mitigation strategy for safety and mission assurance of all NASA’s software



SQ

IV&V

V&V

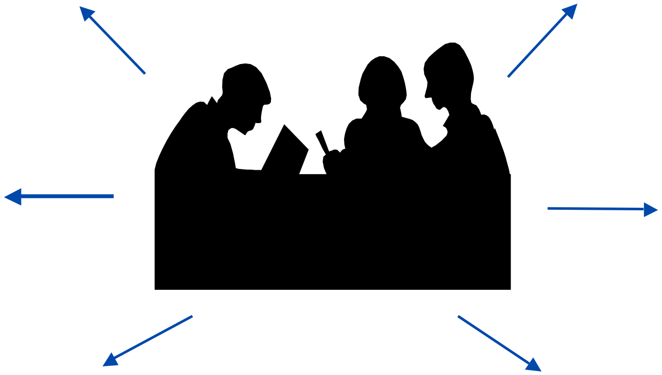
Software Safety

Software Reliability

SQ = Software Quality
V&V = Verification and Validation
IV&V = Independent Verification and Validation

Who are the Practitioners?

Software Assurance practitioners INCLUDE a wide range of personnel, employed throughout the software development life cycle



Software Managers (or PDLs)

Safety Engineers

Software Engineers

Systems Engineers

Software Quality Personnel

IV&V Personnel

Software Assurance personnel aren't just those Software Quality folks!!

What's in it for Me?

Software Assurance:

- **Strives to improve the quality of the product while employing risk mitigation techniques**
- **Focuses on opportunities for early error detection, problem prevention, and risk identification and mitigation**
- **Provides project management insight into the software development processes and products throughout the life cycle**
- **Reviews and assesses interim products – can't build quality in at the end!**
- **Improves the quality of future products/services**

The level of Software Assurance needed is commensurate with the software classification as well as software size, complexity, criticality, and risk

Key Point !

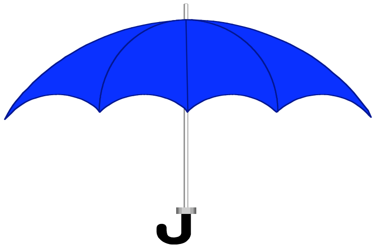
Software Quality

$\neq$

Software Assurance

The Disciplines of Software Assurance

Software Quality



- **Assures that quality is built into the software through the functions of**
  - Software quality assurance
  - Software quality engineering
  - Software quality control
- **Ensures conformance of software life cycle processes and products to requirements, standards, and procedures**
- **Performs process and product activities throughout the life cycle to provide objective insight into the maturity and quality of the software processes and products**
- **Promotes continuous process improvement**

Sample Process and Product Activities

Process

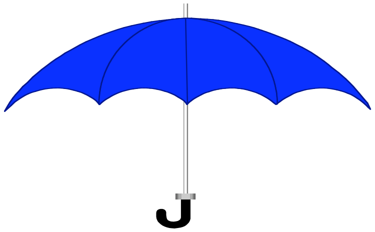
- ✓ All plans (e.g., Configuration Management Plan, Software Management Plan) and procedures are implemented according to specified standards and procedures.
- ✓ Engineering peer reviews and management reviews are conducted and action items are tracked to closure
- ✓ Tests are planned, documented, and conducted using approved test procedures and tools
- ✓ Project risks are documented and addressed in accordance with the risk management plan

Product

- ✓ All required plans are developed in accordance with specified requirements, standards, or procedures
- ✓ All software requirements are documented and traceable from system requirements to design, code, and test
- ✓ Software development records are maintained and up-to-date
- ✓ Configuration baselines are managed, maintained, and accurate
- ✓ Software quality metrics are in place and used to manage the software development effort

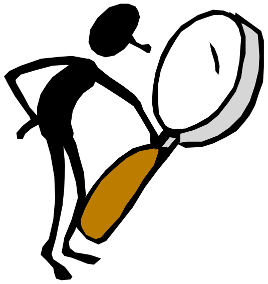
SQ identifies strengths, weaknesses, and areas for improvement!

Independent V&V – IV&V



- **IV&V is Verification and Validation performed by an organization that is technically, managerially, and financially independent of the development organization**
- **IV&V focuses on mission critical software, provides additional reviews and analyses, and provides in-depth evaluations of life cycle products that have the highest level of risk**

Examples:



- Validation of design to meet system needs/requirements
- Traceability of safety critical requirements
- Code analysis of mission-critical software components
- Design analysis of selected critical algorithms

Fundamental Differences

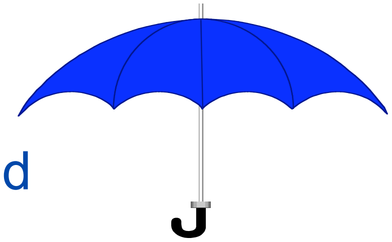
SQ

- Provides **Center**-level services
- Focuses on ALL Project software
- Emphasizes compliance to standards and procedures
- Reviews, monitors and audits all Project processes and products for completeness and accuracy
- Matrixed to the Project as part of the Project Team and provides daily insight/oversight
- Reports to Project and Center Director through S&MA

IV&V

- Provides **Agency**-level services
- Focuses on MISSION CRITICAL Project software
- Emphasizes completeness and correctness of the product
- Reviews, analyzes, and provides in-depth evaluations of life cycle products which have the highest risk
- Independent from the Project and provides analyses and evaluations per IV&V priorities
- Reports to Project, GPMC's, and NASA Headquarters

Verification and Validation (V&V)



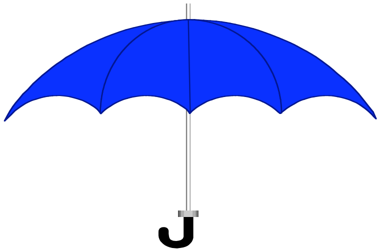
- **Software Verification and Validation**
  - Ensures that software being developed or maintained satisfies functional and performance requirements
  - Ensures that each phase of the development process yields the right products
- **Every participant in the software life cycle process plays a role in some aspect of V&V!**

V&V activities include, but are not limited to:

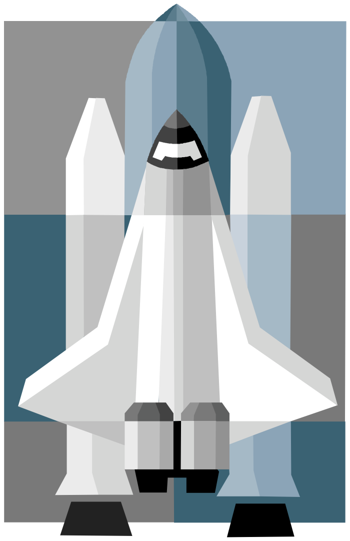
- Analysis of system and software requirements
- Engineering peer reviews (e.g., code walkthroughs)
- Test planning and test execution
- Audits/assessments (e.g., baseline management)

Software Safety

Software Safety is a systematic approach to identifying, analyzing, tracking, mitigating and controlling software hazards and hazardous functions (data and commands) to ensure safer software operation within a system.



Software Safety entails…



Ensuring that software safety requirements are clearly identified, documented, traced and controlled throughout the software lifecycle

Testing of software safety critical components on actual hardware to ensure that the safety requirements were sufficiently implemented and that applicable controls are in place to verify all safety conditions

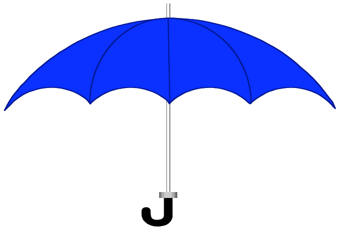
Analysis of the consistency, completeness, correctness and testability of software safety requirements

Continuous analysis of proposed changes on system safety

Software Safety is a function of System Safety!

Software Reliability

Software Reliability is concerned with incorporating and measuring reliability in the products produced throughout the life cycle



Specifically…

- ✓ **Systems Engineering** defines software requirements as they contribute to system robustness
- ✓ **Software Engineering** develops software containing required redundancy and fault tolerance *AND* measures and analyzes software's ability to withstand errors
- ✓ **Software Quality** assures quality metrics/measures are documented, monitored, analyzed and tracked (e.g., error density) *AND* verifies that reliability requirements have been successfully demonstrated

How Do I Get Started??

First Steps…

As a Manager or the PDL, ask the following:

- How much software is predicted to be on the project? How much will be acquired vs. developed in-house?
- What are the software's characteristics and software classification (i.e., Class A – H)?
- What is its criticality? What functions will software control? What hazard controls and mitigations?
- What metrics should be collected? Can they help me measure the maturity and quality of the software product?
- Does the acquisition strategy assure the safety and quality of the software?
- Have I carefully planned for software assurance? Are SQ and IV&V personnel onboard?

Software Classes

Class A	Human Rated Software Systems
Class B	Non-Human Space Rated Software Systems
Class C	Mission Support Software
Class D	Analysis and Distribution Software
Class E	Development Support Software
Class F	General Purpose Computing Software (Multi-Center or Multi-Program/Project)
Class G	General Purpose Computing Software (Singe Center or Project)
Class H	General Purpose Desktop Software

Planning for SQ

For Class B and C software, Code 300 provides Software Quality support to ensure that software assurance activities are performed correctly and to a level commensurate with the software classification

A Software Quality Engineer (SQE):

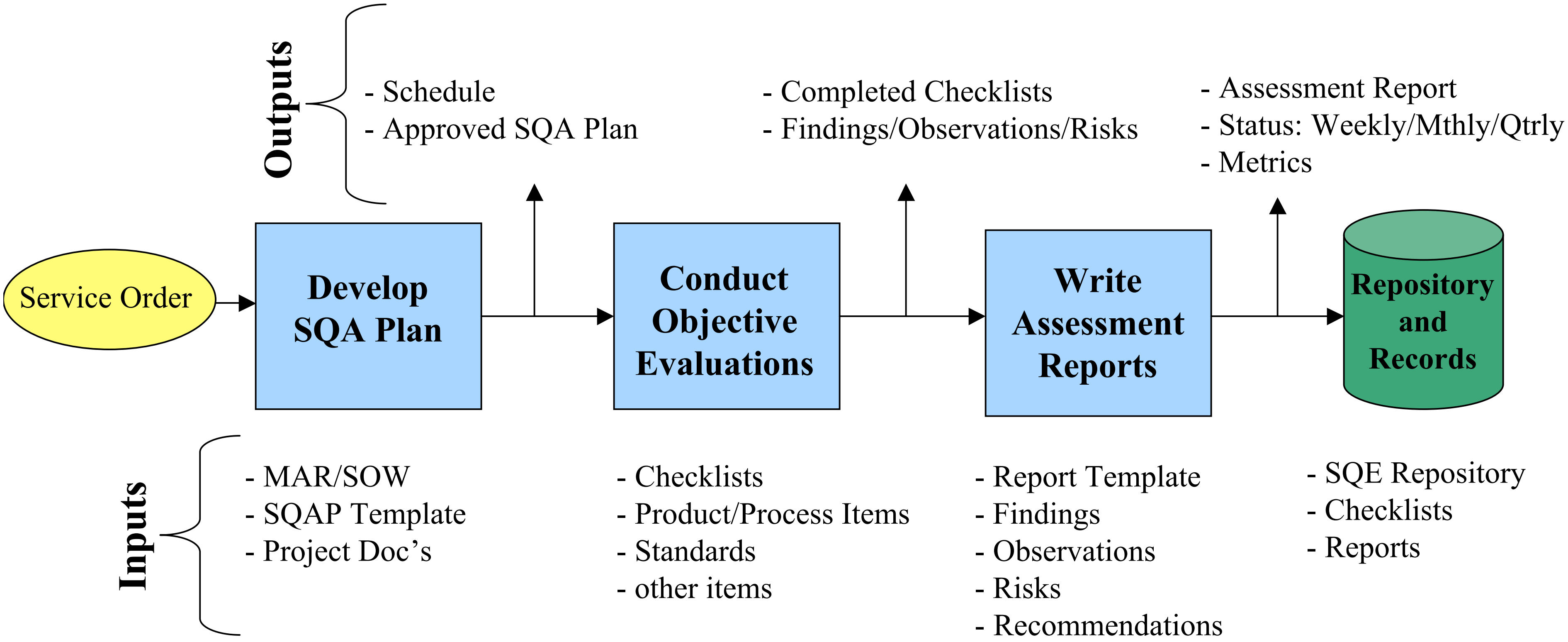
- Matrixed to a mission or software development project during the concept phase
- Participates in the software acquisition process to ensure appropriate software assurance requirements
- Prepares a Software Quality Assurance Plan that documents the goals, processes, and responsibilities required to implement an effective quality program

Planning for SQ – cont.

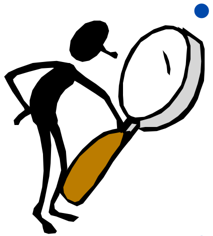
- Conducts independent and objective evaluations of software processes and products throughout the software life cycle *
- Provides project management insight into the quality and maturity of the software *
- Establishes and maintains records of quality assurance activities *
- Interfaces with IV&V to communicate any issues/concerns
- Provides a Quality Status at MORs, ORRs, and FRRs
- Provides support through Operations and Maintenance

***** Software Quality also fulfills the goals and practices of the Level 2 Process and Product Quality Assurance (PPQA)***

Software Quality Process Flow



IV&V Support Criteria

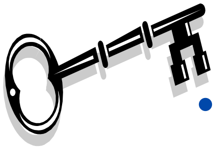


- For most Class B development software (and some Class C software), the NASA IV&V Facility provides IV&V support
- Projects are selected for IV&V based on results from a Software Inventory, Software Assurance Classification Assessment, and a yearly review by an IV&V Board of Directors
- All selected projects are funded by a G&A pool
- IV&V is not “mandatory” for those projects not selected
- IV&V prefers to come onboard during the requirements phase

IV&V Start-up

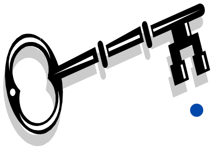
- When selected, IV&V performs a start-up assessment to identify high risk areas and to develop a critical functions list
- IV&V documents proposed IV&V activities in an IV&V Plan (IVVP)
- An IV&V Point of Contact (from the software project) is selected to interface with the IV&V personnel, ensure access to current software products, and address findings and/or recommendations
- Monthly status reports are provided to the project

Keys to a Successful SA Program



- Work with Code 300 to secure Software Quality Engineering (SQE) support
- Perform a Software Assurance Classification Assessment to identify and evaluate the characteristics of software and to determine the software's classification
- Define software assurance requirements early in the life cycle and ensure flow-down to any subcontractors
- Develop a Software Quality Assurance Plan
- Ensure software assurance training for both the acquirer and provider
- Monitor processes throughout the system and software development life cycle

More Keys…

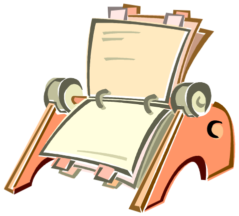


- Evaluate software and deliverables to assure that quality and safety are being built into the products
- Ensure compliance with established standards and procedures
- Establish metrics to help measure quality
- Assure that problems and risks are documented, reported, addressed, and tracked to closure
- Prepare and maintain software assurance records and status reports
- Capture Lessons Learned to improve the quality of future products/services
- Communicate, Communicate, Communicate…

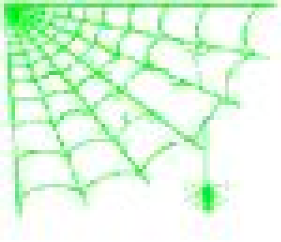
Supplementary Information

GSFC Contacts

- Software Working Group (SWG) Representatives
  - Sally Godfrey 301 286-5706
  - Susan Sekira 301 286-6160
- Center Software Assurance Lead and IV&V Liaison (Code 304)
  - Susan Sekira 301 286-6160
- Systems Assurance and Technology Center (Code 304)
  - Al Gallo, Manager 301 286-3756
- Systems Safety and Reliability Office (Code 302)
  - Karen Fisher, Chief 301 286-7123
- Flight Software Branch (Code 582)
  - Elaine Shell, Head 301 286-2628



Recommended Web Sites



- NASA Software Assurance

  http://software.nasa.gov/
- GSFC Software Assurance

  http://sw-assurance.gsfc.nasa.gov
- NASA Independent Verification and Validation

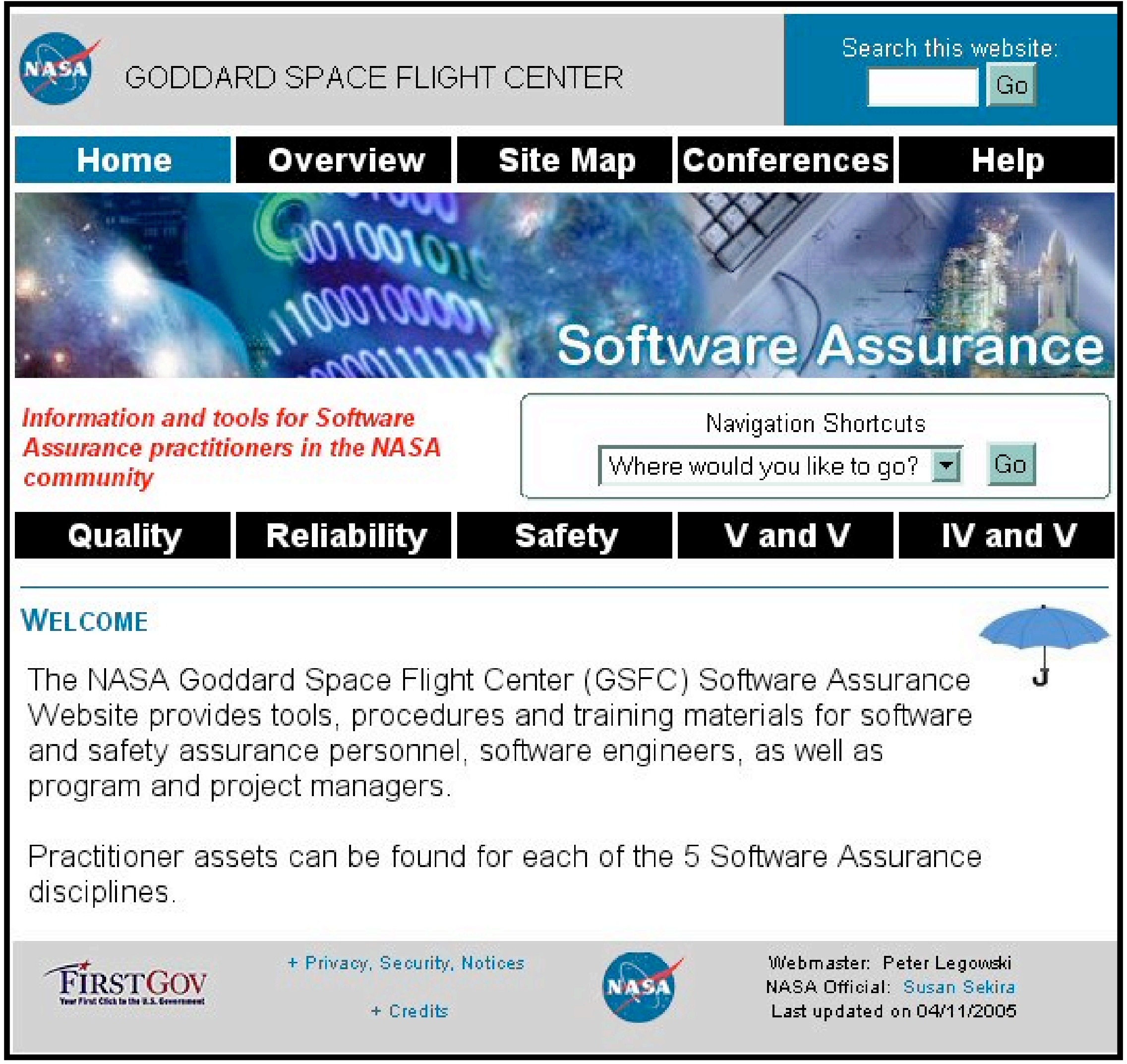
  http://www.ivv.nasa.gov
- GSFC Software Development Process Improvement

  http://software.gsfc.nasa.gov
- NASA Technical Standards

  http://standards.nasa.gov/
- Carnegie Mellon-Software Engineering Institute

  http://www.sei.cmu.edu/

Software Assurance Web Site



Information and tools for Software Assurance practitioners in the NASA community

WELCOME

The NASA Goddard Space Flight Center (GSFC) Software Assurance Website provides tools, procedures and training materials for software and safety assurance personnel, software engineers, as well as program and project managers.

Practitioner assets can be found for each of the 5 Software Assurance disciplines.

Webmaster: Peter Legowski
NASA Official: Susan Sekira
Last updated on 04/11/2005

SA Website was developed as a tool for Practitioners

Links under Quality:

1) **PGs and WIs**
2) **Checklists**
3) **Forms and Templates**
4) **Training**
5) **Presentations**

Recommended Reference Documents

Standard	Description
NASA STD 8739.8	Software Assurance Standard
NASA GB A201	Software Assurance Guidebook
NASA STD 8719.13	Software Safety Standard
NASA GB 8719.13	Software Safety Guidebook
NPD 2820.1	NASA Software Policies
NPR 7150.2	NASA Software Engineering Requirements
ISO/IEC 12207:1995	Software Life Cycle Processes
IEEE-STD-730-2002	IEEE Standard for SQA Plans
IEEE-STD- 982.1-1998	IEEE Standard Dictionary of Measures to Product Reliability Software
SEI-CMM	Software Engineering Institute Capability Maturity Model
SEI-CMMI	Software Engineering Institute Capability Maturity Model Integration

Summary

SA and the Practitioner

- Software Assurance engages full life cycle activities and personnel across many functional areas
- Software Assurance is comprised of 5 disciplines AND SA is not synonymous with SQ
- Software Quality support is provided by Code 300
- IV&V support/funding is determined by HQ
- Software Assurance is everyone's responsibility…

We are all Software Assurance Practitioners

Example SA Activities…

You know you're a SA Practitioner if you participate in:

- Software Assurance Classification Process
- Proposal and contract evaluations
- Development and Analysis of SW Requirements
- Requirements traceability
- Design and code analyses
- Engineering peer reviews
- Test planning and test execution
- Software measurement and trending
- Audits and assessments
- Managed processes and procedures
- Records and configuration management
- Status Reviews with Higher Level Management

Future Topics?

- Software Classification Process
- Software Safety at GSFC
- Tailoring Software Assurance Requirements for Class D software